

REMARKS

Claims 1-28 remain in the application. The claims have been carefully reviewed with particular attention to the points raised in the Office Action. It is submitted that no new matter has been added and no new issues have been raised by the present Request For Reconsideration.

Reconsideration is respectfully requested of the rejection of claims 1, 11 and 28 under 35 U.S.C. § 102(e), as allegedly being anticipated by U.S. Patent No. 6,289,462 to McNabb et al.

Applicant has carefully considered the comments of the Office Action and the cited reference, and respectfully submits that claims 1, 11 and 28 are patentably distinct over the cited reference for at least the following reasons.

The present invention relates to a system for automatic connection to a network. The system also relates to an online advertisement system and to management of digital rights of digital content over the network. The system includes a data card, a data card reader, a data processor and an application program residing in a memory of the data card. The data card may contain user information, including digital rights information. The data card reader may access the user information on the data card, and the data processor may be connected to the network. The application program can be configured to operate in conjunction with a

universal language for creating and controlling digital rights, to manage user rights of digital content available on the network based upon the digital rights information contained on the data card.

McNabb et al., as understood by Applicant, relates to a system and method for providing a trusted server which controls access to the execution of processes by applying file level extended sensitivity label attributes. The attributes are used to restrict execution of processes that are requested by comparing the extended attributes in addition to using standard file permission authorization. The system may also be used to provide controlled execution of commercially available software. See McNabb et al, Abstract. McNabb et al. generally relates to computer systems and operating system design where access, control, rights and privileges are assigned to individual file members, not strictly to the user or process that accesses the computer. See McNabb et al. Column 1, lines 11-14.

The trusted server of McNabb et al. requires that modifications to the operating system are incorporated such that the operation of key components is affected. The key components include: 1) processes; 2) file system objects (including devices, directories, files, etc.); and 3) interprocess communication messages (including packets, shared memory, etc.). On a standard system, each of these has various security attributes, which are

created, managed, and used by the OS itself. When a process attempts to access a file system object, the OS compares various attributes of the process with attributes of the object, and allows or denies access. When a process sends or receives communication messages, the OS verifies that the process is allowed to send and/or receive the message. When objects are created, such as when a file is created or when a message is generated, the OS is responsible for ensuring that the proper attributes are attached to the new object. See McNabb et al., Column 8, line 54 to Column 9, line 4.

With regard to claims 1, 11 and 28, the Office Action quotes Column 1, lines 11-15; Column 3, lines 21-24; and Column 15, lines 54-61 of McNabb et al. The Office Action concedes that McNabb et al. fails to specifically disclose a reader, but contends that in order for a smart card to communicate with an authentication module, such as that discussed at Column 15, lines 54-61 of McNabb et al., that there must be a reader. Applicant respectfully disagrees.

McNabb et al. discloses an authentication module 9 of the trusted server system that can be configured to request a user to provide a user ID and a site-definable authentication response prior to permitting access. Once the user has been authenticated, subsequent web requests can be identified by the upgrade/downgrade enforcer (UDE) as part of an authenticated session and

communication to other restricted partitions can be allowed. See McNabb et al. Column 15, lines 56-61. The authentication device 9 of McNabb et al., however, is only discussed in conjunction with the default website 7 for traffic coming from unprivileged hosts or interfaces. To prevent malicious users from destroying or corrupting the web site, the web pages can be stored in a separate, read-only partition and thus it becomes impossible for a malicious user to exploit holes in commercial web servers or in web applications, such as CGI scripts, to damage the site's web pages. See McNabb et al., Column 15, lines 44-53.

That is, as understood by applicant, the authentication module 9 of McNabb et al. may be used to identify a user from an unprivileged host or interface accessing the system via the default webpage 7.

In contrast, the system of the present application includes a data card having a memory component and an application program resident in the memory component of the data card where the application program is configured to operate in conjunction with a universal language for creating and controlling digital rights. See present specification, p. 24, line 29 to p. 25, line 5.

The user information of the present invention includes digital rights information specific to the user, and the application program resident on the memory component of the data card operates to manage user rights of digital content available on the network

based on the user-specific digital rights. See *id.*, p. 24, line 15 to p. 26, line 16.

More specifically, the application program resident on the memory component of the data card is configured to operate in conjunction with a universal language for creating and controlling digital rights to manage user rights of the digital content available on the network based on the digital rights information specific to the user. See *id.*, p. 24, line 29 to p. 25, line 3.

McNabb et al. fails to show or suggest "an application program resident on the memory component of the data card, the application program being configured to operate in conjunction with a universal language for creating and controlling digital rights, to manage user rights of the digital content available on the network based on the digital rights information specific to the user which is contained in the card as substantially recited in claim 1 of the present application, for example.

In fact, McNabb et al. specifically discloses that privileges are given to programs, not to users (See McNabb, Column 12, lines 61-62). Further, while a specific user may have a right to run certain programs, for example, the user's session is in no way privileged. See McNabb et al., Column 8, lines 65-67.

Furthermore, the smart card of McNabb et al. does not contain an application program which operates in conjunction with a universal language for creating and controlling digital rights.

As understood by Applicant, McNabb et al. fails to disclose or suggest a system for managing digital rights of digital content over a network, comprising a data card which contains user information including digital rights information specific to a user, the data card having a memory component for enabling information to be stored within the data card, a data card reader adapted to access the user information contained on the data card when the data card is in communication therewith, a data processor in communication with the data card reader and adapted to be connected to the network, and an application program resident on the memory component of the data card, the application program being configured to operate in conjunction with a universal language for creating and controlling digital rights, to manage user rights of digital content available on the network based on the digital rights information specific to the user which is contained on the data card, as described above and as substantially recited in independent claim 1 of the present application.

Accordingly, for at least the above-stated reasons, it is respectfully submitted that independent claim 1 is patentable over the cited reference. Independent claim 11, is believed to be patentable over the cited reference for at least similar reasons. Independent claim 28 is also believed to be patentable over the cited reference for at least similar reasons.

Reconsideration is respectfully requested of the rejection of

claims 2 and 12 under 35 U.S.C. § 103(a) as allegedly being unpatentable over McNabb et al. in view of U.S. Patent No. 6,172,674 to Etheredge.

Applicant has carefully considered the comments of the Office Action and the cited references, and respectfully submits that claims 2 and 12 are patentably distinct over the cited references for at least the following reasons.

The Office Action states that "McNabb et al. fails to teach the digital content including one of the following: e-books, e-magazines, e-newsletters, software, games, digital music or digital video." See Office Action, page 3. Etheredge is cited as allegedly showing the missing element. Applicant respectfully disagrees.

Etheredge, as understood by Applicant, relates to an information filtering system that can be used with an electronic program guide. The filtering system provides a variable selection element on a display device. The variable selection element includes a plurality of selection levels, each selection level being associated with a set of selection criteria. Scheduling data is accessed and filtered according to the selection criteria associated with a chosen selection level. The data that passes the filter is displayed to the user. In one embodiment, the selection criteria are graphically displayed to the user. See Etheredge, Column 1, lines 52-62.

Etheredge further discloses that the electronic program guide provides a user with up-to-date television programming information. The user will have customization options to tailor the listings to his or her preferences and to display the listings by different criteria. There may also be search capabilities and short cuts for viewing/recording programs. See Etheredge, Column 3, line 29-34.

As understood by Applicant, Etheredge discloses filtering electronic program guide information in accordance with user preferences.

Applicant respectfully submits, however, that Etheredge does not disclose or suggest digital content including one of the following: e-books, e-magazines, e-newsletters, software, games, digital music or digital video. The program guide information of Etheredge is not an e-book, e-magazine, e-newsletter, software, game, digital music or digital video.

As noted above, it is believed that McNabb et al. fails to show or suggest the system for managing digital rights recited in claim 1 of the present application. Further, Etheredge, either alone or in combination with McNabb et al., fails to show or suggest a system for managing digital rights of digital content over a network, comprising a data card which contains user information including digital rights information specific to a user, the data card having a memory component for enabling information to be stored within the data card, a data card reader



adapted to access the user information contained on the data card when the data card is in communication therewith, a data processor in communication with the data card reader and adapted to be connected to the network, and an application program resident on the memory component of the data card, the application program being configured to operate in conjunction with a universal language for creating and controlling digital rights, to manage user rights of digital content available on the network based on the digital rights information specific to the user which is contained on the data card, as described above and as substantially recited in independent claim 1 of the present application.

Accordingly, for at least the above-stated reasons, it is respectfully submitted that independent claim 1, and the claims depending therefrom, including claim 2, are patentable over the cited references. Independent claim 11, and the claims depending therefrom, including claim 12, are believed to be patentable over the cited references for at least similar reasons.

Reconsideration is respectfully requested of the rejection of claims 3-7, 9, 10, 13-17, 19 and 20 under 35 U.S.C. § 103(a), as allegedly being unpatentable over McNabb et al. in view of U.S. Patent No. 6,044,349 to Tolopka et al.

Applicant has carefully considered the comments of the Office Action and the cited references, and respectfully submits that claims 3-7, 9, 10, 13-17, 19 and 20 are patentably distinct over

the cited references for at least the following reasons.

With regard to claims 5-7 and 15-17 the Office action contends that McNabb et al. teaches a data card containing access rights information and usage information. Furthermore, the Office action contends that McNabb et al. discloses authorizing a user following a match of the information stored on the data card and information inputted by the user. In addition, the Office Action contends that McNabb et al. discloses further usage rights including read only rights. See Office Action, page 5. Applicant respectfully disagrees.

As noted above, McNabb et al. discloses an authentication module that can be configured to request a user ID and a site-definable authentication response such as a password, a biometric device, a smart card or an access token check. See McNabb et al., Column 15, lines 55-57.

McNabb et al. does not disclose a data card containing access rights information and usage information, as substantially recited in claims 5 and 15 of the present application. Further, McNabb et al. fails to show or suggest authorizing a user following a match of the information stored on the data card and information inputted by the user as substantially recited in claims 6 and 16 of the present application. McNabb et al. simply discloses requesting a user to input ID information and a site-definable authentication response which may include a smart card. McNabb et al. does not

disclose matching information inputted by the user to information stored on the smart card. In addition, McNabb et al. does not specifically disclose usage rights including read only rights as substantially recited in claims 7 and 17 of the present application.

The Office Action concedes that "McNabb et al. fails to specifically teach inputting personal identification information for encryption and storage on the data card." See Office Action page 5. Tolopka et al. is cited as allegedly showing the missing element. Applicant respectfully disagrees.

Tolopka et al. as understood by Applicant, relates to a portable storage medium used to store data and provide access to information from an information dissemination system (IDS). The storage medium can store one or more location/key pairs. Each of the location/key pairs designates a particular IDS location as well as an access key to the particular IDS. See Tolopka et al., Column 2, lines 5-10.

The Office Action cites Column 1, lines 53-60 and Column 3, line 66 to Column 4 line 7 of Tolopka et al. as related to claims 3, 4, 13 and 14 of the present application. While Tolopka et al., may disclose that smart cards are used to increase computer security and that a computer password can be encrypted and stored in a card's memory, Tolopka et al. fails to show or suggest a system for managing digital rights over a network wherein upon the

initial use of the data card, the user is prompted to initiate the data card by inputting personal information and authentication information into the data processor for encryption on the data card as is substantially recited in claims 3 and 13 of the present application, for example. Tolopka et al. merely discloses that a computer password can be encrypted on a smart card and that a smart card may include personal information. Neither Tolopka et al. nor McNabb et al. teach or suggest prompting a user to initiate the data card as described above.

As previously mentioned, it is believed that McNabb et al. fails to show or suggest the system for managing digital rights of claim 1 of the present application. Furthermore, it is respectfully submitted, that Tolopka et al., either alone or in combination with McNabb et al., fails to disclose or suggest a system for managing digital rights of digital content over a network, comprising a data card which contains user information including digital rights information specific to a user, the data card having a memory component for enabling information to be stored within the data card, a data card reader adapted to access the user information contained on the data card when the data card is in communication therewith, a data processor in communication with the data card reader and adapted to be connected to the network, and an application program resident on the memory component of the data card, the application program being

configured to operate in conjunction with a universal language for creating and controlling digital rights, to manage user rights of digital content available on the network based on the digital rights information specific to the user which is contained on the data card, as described above and as substantially recited in independent claim 1 of the present application.

Accordingly, for at least the above-stated reasons, it is respectfully submitted that independent claim 1, and the claims depending therefrom, including claims 3-7, 9 and 10, are patentable over the cited references. Independent claim 11, and the claims depending therefrom, including claims 13-17, 19 and 20, are believed to be patentable over the cited references for at least similar reasons.

Reconsideration is respectfully requested of the rejection of claims 8 and 18 under 35 U.S.C. § 103(a), as allegedly being unpatentable over McNabb et al. in view of U.S. Patent Publication No. 2002/0175207 to Kashef et al.

Applicant has carefully considered the comments of the Office Action and the cited references, and respectfully submits that claims 8 and 18 are patentably distinct over the cited references for at least the following reasons.

The Office Action concedes that McNabb et al. fails to teach tracking subsequent use of the digital content by the user. See Office Action, page 7. Kashef et al. is cited as providing this

missing element. Applicant respectfully disagrees.

Kashef et al., as understood by Applicant, relates generally to smart card terminals. More specifically, Kashef et al. relates to a terminal software architecture that allows terminal applications to be portable to multiple terminals. See Kashef et al., page 1, paragraph 0002. In one embodiment, a terminal software architecture and associated terminal for accepting a smart card implementing a card application of a merchant is presented. Through the use of this terminal architecture, terminal applications and card applications can be developed in parallel such that the resulting applications are guaranteed to be compatible. Moreover, a terminal application designed for use with a specific card application can be used with different terminals. See Kashef et al., page 3, paragraph 0035.

The Office Action cites Page 1, paragraph 0003 of Kashef et al. which discloses that businesses currently make use of loyalty programs that reward frequent purchases of the business' products or services and that loyalty programs may be implemented using smart cards in conjunction with a terminal at a loyalty operator's place of business. See Kashef et al. page 1, paragraph 0003.

While Kashef et al. may disclose tracking purchases of a user in a loyalty program, Kashef et al. does not show or suggest an application program that is configured to track subsequent use of the digital content by the user, as substantially recited in claims

8 and 18 of the present application. Kashef et al. discloses tracking subsequent transactions of the user, not subsequent uses of digital content.

Further, it is respectfully submitted that Kashef et al., either alone or in combination with McNabb et al., fails to disclose or suggest a system for managing digital rights of digital content over a network, comprising a data card which contains user information including digital rights information specific to a user, the data card having a memory component for enabling information to be stored within the data card, a data card reader adapted to access the user information contained on the data card when the data card is in communication therewith, a data processor in communication with the data card reader and adapted to be connected to the network, and an application program resident on the memory component of the data card, the application program being configured to operate in conjunction with a universal language for creating and controlling digital rights, to manage user rights of digital content available on the network based on the digital rights information specific to the user which is contained on the data card, as described above and as substantially recited in independent claim 1 of the present application.

Accordingly, for at least the above-stated reasons, it is respectfully submitted that independent claim 1, and the claims depending therefrom, including claim 8, are patentable over the

cited references. Further, it is respectfully submitted that independent claim 11, and the claims depending therefrom, including claim 18, are patentable over the cited art for at least similar reasons.

Reconsideration is respectfully requested of the rejection of claim 21 under 35 USC § 103(a), as allegedly being unpatentable over McNabb et al. in combination with Tolopka et al. and further in view of Kashef et al.

Applicant has carefully considered the comments of the Office Action and the cited references, and respectfully submits that claim 21 is patentably distinct over the cited references for at least the following reasons.

The Office Action contends that it would have been obvious to one of ordinary skill in the art at the time of the invention was made to include the ability to track user's digital content use on the application program located on the data card, and that the data card disclosed by the combination of McNabb et al. and Tolopka et al. includes user information needed to permit access to various types of digital content where the user inputs identification information onto the data card. The Office Action further contends that one would have been motivated to include the data card system taught by the combination of McNabb et al. and Tolopka et al., and a tracking system as taught by Kashef et al. in order to reward the user with free digital content. Applicant respectfully disagrees.



As noted above neither McNabb et al. nor Kashef et al. teach or suggest an application program adapted to track the subsequent use of the digital content by the user.

Further, it is respectfully submitted that none of McNabb et al, Tolopka et al., or Kashef et al, either alone or in combination, teach or suggest a system for managing digital rights of digital content over a network, comprising a data card which contains user information including digital rights information specific to a user, the data card having a memory component for enabling information to be stored within the data card, a data card reader adapted to access the user information contained on the data card when the data card is in communication therewith, a data processor in communication with the data card reader and adapted to be connected to the network, and an application program resident on the memory component of the data card, the application program being configured to operate in conjunction with a universal language for creating and controlling digital rights, to manage user rights of digital content available on the network based on the digital rights information specific to the user which is contained on the data card, to track subsequent use of the digital content by the user, to update an account balance of the user stored on the memory component of the data card for payment of fees for accessing and using the digital content, and to maintain financial information for an owner of the digital content as

recited in claim 21 of the present application.

Reconsideration is respectfully requested of the rejection of claims 22-27 under 35 USC § 103(a), as allegedly being unpatentable over McNabb et al. in combination with Tolopka et al. and Kashef et al. and in further view of Etheredge.

Applicant has carefully considered the comments of the Office Action and the cited references, and respectfully submits that claims 22-27 are patentably distinct over the cited references for at least the following reasons.

The Office Action contends that McNabb et al. discloses a data card containing access rights information and usage rights information and authorizing a user following a match of the information stored on the data card and information inputted by the user and further usage rights information including read-only rights. The Office Action concedes that the combination of teachings fails to specifically teach that the digital content includes at least one of e-books, e-magazines, software, digital music and digital video. Etheredge is cited as allegedly disclosing this missing element.

The Office Action contends that it would have been obvious to one of ordinary skill in the art at the time of the invention to include, user approved access to digital content via use of a user inputted data card, including a tracking system wherein the digital content includes e-books, etc. (as taught by Etheredge). The

Office Action further concedes that McNabb et al. in combination with Tolopka et al and Kashef et al. do not specifically teach the digital content being in the form of e-books, but that one would be motivated to include e-books as a form of digital content in order to not only guard against viewing a web page as taught be McNabb et al., but also guard against unauthorized access to other forms of digital content such as e-books. Applicant respectfully disagrees.

As noted above, neither McNabb et al. nor Etheredge show or suggest digital content including at least one of an e-book, e-magazine, software, game, digital music or digital video. Similarly Tolopka et al. and Kashef et al. fail to show or suggest digital content including at least one of an e-book, e-magazine, software, game, digital music and digital video. The program guide information of Etheredge is not an e-book, e-magazine, software, game, digital music or digital video.

Furthermore, as noted above, it is believed that none of McNabb et al., Tolopka et al., or Kashef et al, either alone or in combination, teach or suggest a system for managing digital rights as recited in claim 2 of the present application. Further, it is respectfully submitted that none of McNabb et al., Tolopka et al., Kashef et al. or Etheredge show or suggest a system for managing digital rights of digital content over a network, comprising a data card which contains user information including digital rights information specific to a user, the data card having a memory

component for enabling information to be stored within the data card, a data card reader adapted to access the user information contained on the data card when the data card is in communication therewith, a data processor in communication with the data card reader and adapted to be connected to the network, and an application program resident on the memory component of the data card, the application program being configured to operate in conjunction with a universal language for creating and controlling digital rights, to manage user rights of digital content available on the network based on the digital rights information specific to the user which is contained on the data card, to track subsequent use of the digital content by the user, to update an account balance of the user stored on the memory component of the data card for payment of fees for accessing and using the digital content, and to maintain financial information for an owner of the digital content as recited in claim 21 of the present application.

Accordingly, for at least the reasons discussed above, it is respectfully submitted that claim 21, and the claims depending therefrom, including claims 22-27 are patentably distinct over the cited references.

Should the Examiner disagree, it is respectfully requested that the Examiner specify where in the cited document there is a basis for such disagreement.

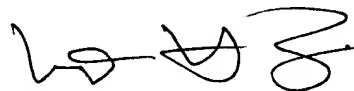
The Office is hereby authorized to charge any fees which may

64482

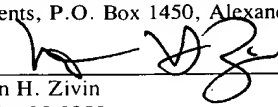
be required in connection with this Request For Reconsideration and to credit any overpayment to Deposit Account No. 03-3125.

Favorable reconsideration is earnestly solicited.

Dated: January 18, 2005



I hereby certify that this paper is being deposited this date with the U.S. Postal Service as first class mail addressed to: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450

  
Norman H. Zivin  
Reg. No. 25,3855

1/18/05  
Date

Norman H. Zivin  
Reg. No. 25,385  
c/o Cooper & Dunham LLP  
1185 Avenue of the Americas  
New York, NY 10036  
(212) 278-0400  
Attorney for Applicant